UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ANNABELLE ZARATZIAN, Plaintiff, v. ADEL RAMSEY ABADIR, and LARRY M. CARLIN, Defendants.	10-CIV-09049 (VLB)

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT ADEL RAMSEY ABADIR'S MOTION FOR SUMMARY JUDGMENT

Ballard Spahr Stillman & Friedman LLP
425 Park Avenue
New York, NY 10022
(212) 223-0200

Attorneys for Defendant Adel Ramsey Abadir

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

OTHER AUTHORITIES

Defendant Adel Ramsey Abadir respectfully submits this memorandum of law in support of his motion for summary judgment pursuant to Rule 56 of the Federal Rules of Civil Procedure.

PRELIMINARY STATEMENT

This action is a misguided attempt to bring the parties' long-pending divorce and custody litigation into federal court. As this Court is aware, Plaintiff, Dr. Annabelle Zaratzian, contends that Dr. Abadir, her ex-husband, set up her e-mail account to "auto-forward" her incoming e-mails to him, and that he continued to receive those e-mails after the parties separated. Plaintiff alleges that Dr. Abadir violated two criminal statutes which provide private causes of action -- the "Wiretap Act" and the "Stored Communications Act" (see Plaintiff's Second Amended Complaint ("SAC" or "Complaint"), Counts One and Two) -- and she asserts various state law claims.[1]

In essence, Plaintiff claims that Dr. Abadir's passive receipt of e-mails constituted both "wiretapping" and "computer hacking." But this conduct does not rise to the level of criminality necessary to violate the statutes. Indeed, exhaustive research has failed to uncover a single case where the authorized setting of an account feature somehow became unlawful without any further action by the defendant, or where liability was otherwise recognized on remotely comparable facts. To the contrary, every case finding a violation of these Acts involves the type of nefarious conduct that is absent here, such as computer hacking or the installation of "keylogger" software on a computer to steal the victim's password.

---

[1] Counts Three and Four of the SAC allege a violation of New York's wiretap statute and a trespass to chattels, respectively. These claims have been dismissed by stipulation. The only remaining state claim is Count Five, constructive fraud by fiduciary, which is addressed below in Point II.

The undisputed evidence established in discovery confirms that summary judgment is warranted. The Wiretap Act claim fails because (i) Plaintiff gave valid consent to Dr. Abadir by sharing her password, and she never withdrew that consent; (ii) there was no unlawful "interception" under the narrow statutory definition of that term; and (iii) the statute of limitations has run because Plaintiff, by her own admission, suspected that Dr. Abadir was reading her e-mails more than two years before she filed her Complaint, and thus she was on "inquiry notice" sufficient to trigger the running of the limitations period. The Stored Communications Act claim fails for many of the same reasons, but also because Dr. Abadir never "accessed" Plaintiff's account; rather, he logged onto his own account and read his own e-mail. Finally, the remaining state claim (constructive fraud by fiduciary) is defective, and the request for an injunction (Count Six) should be dismissed because the underlying substantive claims lack merit.

THE FACTS

The pertinent facts are set forth in the accompanying Rule 56.1 statement of undisputed facts, which is incorporated herein.

ARGUMENT

The claims here should be dismissed because there are no material facts in dispute and Dr. Abadir is entitled to summary judgment as a matter of law. See State Emp. Bargaining Agent Coalition v. Rowland, 718 F.3d 126, 131-32, (2d Cir. 2013)(summary judgment should be granted where, "construing the evidence in the light most favorable to the nonmoving party, 'there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law'")(quoting Fed. R. Civ. Proc. 56(a)).

POINT I

THE COURT SHOULD GRANT SUMMARY JUDGMENT ON THE WIRETAP ACT AND STORED COMMUNICATIONS ACT CLAIMS

A. Overview of the Wiretap and Stored Communications Acts

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"). Title I of the ECPA amended the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), 18 U.S.C. §2510, et seq., which prohibits a person from "intentionally intercept[ing] . . . any wire, oral, or electronic communication." United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996)(citations omitted). Title II of the ECPA (the "Stored Communications Act" or "SCA"), 18 U.S.C. §2701(a), et seq., prohibits a person from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided," or doing so in excess of one's authorization, and thereby obtaining access to an electronic communication "while it is in electronic storage." The SCA "was primarily designed to provide a cause of action against computer hackers." State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995). Accord, Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495-96 (D. Md. 2005).

Both Acts are criminal statutes that provide private rights of action. See 18 U.S.C. §2520 (Wiretap Act); 18 U.S.C. §2707 (SCA). It is precisely because of their criminal nature that they are construed strictly. Under the SCA, for example, where a civil violation is alleged, liability exists only when the defendant has acted with a heightened mental state. Section 2707(a) requires that "the conduct constituting the violation [must be] engaged in with a knowing or intentional state of mind." The term "intentional" as used in the statute "is narrower than the dictionary definition of 'intentional' [and] means more than one voluntarily engaged in

conduct or caused a result." Butera & Andrews v. IBM Corp., 456 F. Supp. 2d 104, 109 (D.D.C. 2006)(citation omitted). That is, the "conduct or the causing of the result must have been the person's conscious objective." Id. See also Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001)(act is done "intentionally" for purposes of Wiretap Act "if it is the conscious objective of the person to do the act or cause the result").

It is also because they are primarily criminal prohibitions that the "rule of lenity" applies, and courts therefore "interpret any ambiguity in the statute[s] in [defendant's] favor." Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004)("Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."); Citron v. Citron, 722 F.2d 14, 16 (2d Cir. 1983)(rejecting argument that less needs to be shown for civil Wiretap Act claim than for criminal prosecution since it "does [not] seem logical that the same term . . . in the same statute, §2511, should have any different meaning when applied directly to a criminal violation than when the same violation is incorporated by reference to establish civil liability"); Clarity Services v. Barney, 698 F. Supp. 2d 1309, 1316 (M.D. Fla. 2010)(applying more defendant-favorable definition of "authorization" under rule of lenity and thereby dismissing civil SCA case).

As shown further below, the two Acts are mutually exclusive under the circumstances alleged here. If an electronic communication is in transit it may be "intercepted" in violation of the Wiretap Act, but it cannot be considered "stored" for purposes of the SCA. Conversely, stored computer information may be unlawfully "accessed" in violation of the SCA, but it cannot be "intercepted" for purposes of the Wiretap Act. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002). The great weight of authority has held that the SCA is

broader and that close cases tend to fall within its parameters rather than within the narrower confines of the Wiretap Act.

B. There was No Wiretap Act Violation Here

For several reasons, the Court should grant summary judgment on the Wiretap Act claim, Count One of the SAC. First, there is no evidentiary dispute that Plaintiff consented to the monitoring by virtue of her openly sharing her password with her then-husband. Moreover, Plaintiff never revoked consent, and the law does not recognize an implied revocation under the facts here. Second, there was no "interception" of any e-mail messages under the Act because the e-mails were obtained after they reached the destination server and were obtained from "storage." The allegations, if anything, thus implicate the Stored Communications Act. Finally, the statute of limitations on the claim has run.

i. Legal Background

Any analysis of a Wiretap Act claim in the context of family litigation must begin with Anonymous v. Anonymous, 558 F.2d 677, 677 (2d Cir. 1977), in which the Second Circuit interpreted the Act narrowly -- and even counter to its plain language -- so as to discourage making federal crimes out of domestic disputes. The court there addressed the scope of interspousal liability under the Wiretap Act. It first observed that the Fifth Circuit, in Simpson v. Simpson, 490 F.2d 803 (5th Cir. 1974), had narrowly construed the statute to avoid finding liability where the husband, suspecting that his wife was unfaithful, had taped her phone calls in their home. The Fifth Circuit had held that "[t]he naked language of Title III, by virtue of its inclusiveness, reaches this case, [but] we are of the opinion that Congress did not intend such a farreaching result, one extending into areas normally left to states, those of the marital home and domestic conflicts." Id. at 805. The Fifth Circuit placed great emphasis on the legislative

history of the Act as well as the fact that, as a criminal statute, it should be "strictly construed, to avoid ensnaring behavior that is not clearly proscribed." Id. at 809.

Following Simpson, the Anonymous Court decided that an ex-husband who placed a recording device on his home phone to capture his wife's calls to his children did not violate the Act. It observed that "nobody wants to make it a crime for a father to listen in on his teenage daughter or some such related problem." 558 F.2d at 679 (quoting testimony before the House on the bill that led to the Act). The court distinguished other cases finding domestic wiretapping violations because they "were criminal prosecutions rather than civil damages actions brought pursuant to 18 U.S.C. §2520." Id. at 679 n.6. The Court concluded as follows:

> The facts in the instant case . . . present a purely domestic conflict [--] a dispute between a wife and her ex-husband over the custody of their children[,] a matter clearly to be handled by the state courts. We do not condone the husband's activity in this case, nor do we suggest that a plaintiff could never recover damages from his or her spouse under the federal wiretap statute. We merely hold that the facts of this case do not rise to the level of a violation of that statute.

Id. at 679.

The couple in Janecka v. Franklin, 684 F. Supp. 24 (S.D.N.Y. 1987), aff'd, 843 F.2d 110 (2d Cir. 1988), was already divorced when the husband taped his wife's calls to his daughter, but Judge Sand refused to distinguish Anonymous on this ground. See id. at 26 ("Anonymous turned on the nature of the interception, i.e., of conversations on one's own telephone installed in one's own home, and the nature of the underlying controversy")(emphasis added). In dismissing the complaint, he concluded that "[n]othing more clearly belongs in state, not federal, court than a contested custody proceeding." Id. The Second Circuit affirmed "substantially for the reasons stated in the opinion of the district court." 843 F.2d at 111. See also Lizza v. Lizza, 631 F. Supp. 529, 533 (E.D.N.Y. 1986)(dismissing claims of wife and non-

family member whose calls had also been intercepted, finding it "irrelevant" whether "plaintiff is a family member who used the telephones in the family home or a third party who had conversations with a person using such telephone lines").

Although Anonymous may be the minority view regarding interspousal claims under the Wirteap Act, it remains good law in the Second Circuit. The case underscores that the court strongly believes that allegations of surveillance made by aggrieved ex-spouses in the midst of divorce or custody proceedings belong in the state tribunals. At the very least, it stands for the proposition that federal claims such as those made here should be viewed through a narrow prism.

ii. Plaintiff Cannot Establish Lack of Consent

Plaintiff's Wiretap Act claim fails because the undisputed evidence demonstrates that Dr. Abadir had Plaintiff's consent to access all aspects of her e-mail account. See 18 U.S.C. §2511(2)(d)("prior consent" of one party is defense to claim of unlawful interception under Wiretap Act). Since that consent was never withdrawn, Dr. Abadir cannot be held liable under the Act.[2]

a. The Facts

The record is clear that Plaintiff was not computer savvy, so in 2001 she had her husband set up her e-mail account and create her password. She testified that Dr. Abadir entered into the contract with Cablevision to establish internet and e-mail service on behalf of himself

[2] We discuss "consent" (under the Wiretap Act) and "authorization" (under the SCA) somewhat interchangeably below because "[f]ederal courts have equated 'consent' under the Wiretap Act with 'authorization' under the Stored Communications Act." Pietrylo v. Hillstone Restaurant Group, 2008 WL 6085437, at *3 (D.N.J. July 25, 2008). See also In re Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001)("In reviewing the case law and legislative histories of Title II [SCA] and the Wiretap Act, we can find no difference in their definition [ ] of . . . 'authorize' (Title II) and 'consent' (Wiretap Act).").

and Plaintiff. (Zaratzian Depo. at 14 ln. 7-24) Until that time, Plaintiff did not have an e-mail account, and she only opened one at Dr. Abadir's suggestion. (Id. at 14 ln. 23-24, 17 ln 3-15). In fact, she had never used e-mail before. (Id. at 28 ln. 2-4) Dr. Abadir "set up [her] account," although she had "no idea" specifically what he did. (Id. at 14 ln. 20 to 15 ln. 2) To do so, he used a computer that was either "in the upstairs study or in the children's study." (Id. at 26 ln. 12-13) When Dr. Abadir asked her what password she wanted to use, she replied, "'I have no idea for a password,'" and thus "he came up with a password" for her. (Id. at 25 ln. 16-18) At that time, Plaintiff did not have her own computer in the house (id. at 26 ln. 14-20)("there would have been one [computer] for the children and one for him"), and she "almost never" used the family computers (id. at 27 ln. 12). Plaintiff accessed her new e-mail account only from a shared house computer, and only "occasionally." (Id. at 35 ln. 13 to 36 ln. 5) She never told her husband that he could not access her account. (Id. at 34 ln. 6-9). And she does not recall changing the password that Dr. Abadir had set for her, at least until the couple separated in September 2005. (Id. at 28 ln. 9 to 30 ln. 2)

b. The Law of Consent Under the Wiretap Act

The Second Circuit has held that consent under the Wiretap Act is "to be construed broadly" and includes "implied" consent. United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987). Accord, Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990)(under Wiretap Act, "consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights"); George v. Carusone, 849 F. Supp. 159, 164 (D. Conn. 1994)("Because Congress intended a broad construction of the consent exception, courts resoundingly have recognized the doctrine of implied consent.")(citing Amen and other cases); In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d at 514 n.23.

The question of consent and authorization has produced its own particular jurisprudence in the recent technology age, as courts have grappled with privacy boundaries on shared computers in the home and overlapping family internet accounts. The issue has arisen in Wiretap Act and SCA cases (often spouses or partners suing each other claiming spying) and in criminal cases (a defendant challenging a police computer search based on third-party consent). The guiding principle is that "[w]here a party consents to another's access to its computer network, it cannot claim that such access was unauthorized." Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000). The defendant's motive for intercepting is "not relevant." Abraham, 237 F.3d at 391. Accord, In re State Police Litig. 888 F. Supp. 1235, 1263 (D. Conn. 1995); see also Lasco Foods, Inc. v. Hall & Shaw Sales, Marketing & Consulting, LLC, 600 F. Supp. 2d 1045, 1050 (E.D. Mo. 2009)(irrelevant under SCA that defendants allegedly obtained information for "improper purposes" where they had authority to access system).

In domestic cases, the law can be distilled to the following simple rule: consent exists where a family member does not password-protect his or her information, either by failing to use a password or by sharing the password with another. See United States v. Alter, 2012 WL 3916513, at *7 (N.D. Ind. Sept. 7, 2012)("[s]everal circuits" have held that consent turns on whether one user had protected files "with a password that the other user does not know"); Richard C. Turkington, Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes Under Federal and State Wiretap and Stored Communications Acts and the Common Law Privacy Intrusion Tort, 82 Neb. L. Rev. 693, 719 (2004)(reasonableness of privacy expectation depends on whether spouses "share passwords" to e-mail accounts).

In the leading case of Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001), plaintiffs Trulock and Conrad shared a computer in the bedroom of their townhouse, but maintained "separate, password-protected files on the hard drive" and "did not know each other's passwords and could not, therefore, access each other's private files." Id. at 398. Nevertheless, FBI agents searched Trulock's computer files after obtaining Conrad's consent. Trulock brought a Bivens action challenging the search. The court held:

> Conrad lacked authority to consent to the search of Trulock's files. Conrad and Trulock both used a computer located in Conrad's bedroom and each had joint access to the hard drive. Conrad and Trulock, however, protected their personal files with passwords; Conrad did not have access to Trulock's passwords. Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files.

Id. at 403 (emphasis added). See also id. ("By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. Moreover, because he concealed his password from Conrad, . . . Trulock had a reasonable expectation of privacy in the password-protected computer files and Conrad's authority to consent to the search did not extend to them.")(emphasis added).

The facts in State v. Rice, 2012 WL 1718035 (Ohio Ct. App. May 16, 2012), stand in contrast, and the court there accordingly reached the opposite result. At issue was the father's challenge to the validity of the mother's consent to a police search of a laptop used throughout the household. Although the laptop had a password, "it was a common password for one main user and the entire family knew the password." Id. at *3. The court explained that the "key factors" in analyzing the validity of the search were "'whether the consenting third party in fact used the computer, whether it was located in a common area accessible to other occupants of the premises, and -- often most importantly -- whether the defendant's files were password

protected.'" Id. (quoting United States v. Clutter, 674 F.3d 980, 984 (8th Cir. 2012))(emphasis added). Since the computer was "jointly accessed by the entire family," the court concluded, the mother had authority to consent to its search. Id.

Another oft-cited case is White v. White, 781 A.2d 85 (N.J. Super. Ct. 2001), in which the plaintiff (husband) invoked the identical New Jersey state wiretap statute. The couple there was divorced but continued to live in the same house. The wife hired a firm to copy the husband's AOL e-mails, which had been automatically saved to the computer's hard drive. The court held that this was not unauthorized, explaining that "'without authorization' means using a computer from which one has been prohibited, or using another's password or code without permission," and although the wife "did not often use the family computer, [she] had authority to do so." Id. at 90 (quoting Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817 (E.D. Mich. 2000)).

United States v. Cole, 2008 WL 2952762 (D. Me. July 24, 2008), also presented facts very similar to those here. Presby and Cole were life partners who shared a computer, though Presby was the technologically savvy one. Presby selected the computer and paid for it, set up the couple's separate user account, and was the primary administrator for the computer. As such, "he had ready access to Cole's desktop user account, notwithstanding the password protection that may have restricted access to Cole's account by someone other than Presby or Cole." Id. at *4. In light of the "'what's mine is yours' ethos . . . that extended to the computer in question," the court upheld Presby's consent to a police search of the computer. Id.[3]

---

[3] For other similar cases, see, e.g, United States v. Stabile, 633 F.3d 219, 232-33 (3d Cir. 2011)("The failure to use password protection indicates that Stabile relinquished his privacy in the contents of the computer."); United States v. Aaron, 33 F. App'x 180, 184 (6th Cir. 2002)(although live-in girlfriend had not used defendant's new computer, she still had authority to consent to its search since he did not "restrict[] her access with password protections"); United

c. Dr. Abadir had Plaintiff's Consent to Access her E-mail Account

What occurred here is a classic example of consent. Plaintiff allowed her husband to establish her e-mail account and set her password, and thus granted him wholesale authorization to access her account as he saw fit. As the de facto administrator of the account, he could access her in-box (which contained the forwarded e-mails) as well as her out-box (which did not); he could adjust her settings; and he could even log-on as her and communicate with others thusly. Whether his purpose in setting the auto-forward rule was laudable (to make sure the children's schedules were properly disseminated, as Dr. Abadir contends), or nefarious (to snoop, as Plaintiff argues), is irrelevant under the law. In re State Police Litig., 888 F. Supp. at 1263. What matters is that his wife specifically allowed him to see and monitor her entire e-mail account.[4]

Finally, and perhaps most importantly, as the owner of the account, Dr. Abadir did not even need his wife's consent, since Cablevision, the internet service provider, authorized his access. See Cornerstone Consultants, Inc. v. Production Input Solutions, L.L.C., 789 F. Supp. 2d 1029, 1051 (N.D. Iowa 2011)("a 'provider's' authorization would make a 'user's' lack of authorization of no consequence"). The Court therefore need not even reach the issue.

A recent case from this district makes the point. The defendant in Connelly v. Wood-Smith, 2012 WL 7809099 (S.D.N.Y. May 14, 2012), report and recommendation adopted, 2013 WL 1285168 (S.D.N.Y. March 28, 2013), was a trustee who controlled an art gallery that

---

States v. Mitchell, 2013 WL 3808152, at *30 (M.D. Fla. July 22, 2013)(common owner's consent to search iPhone and iPad was valid where items were not password-protected).

[4] We note, however, that Dr. Abadir's position is more logical. If his purpose were improper, presumably he would have set the account to forward his wife's outgoing as well as incoming e-mail. That he chose only the latter underscores that his purpose was to make sure that e-mails regarding the children's schedule that were sent only to his wife did not go unseen. (Abadir Depo. 19 ln. 14-24) Moreover, Plaintiff has offered no improper motive for Dr. Abadir to monitor her incoming e-mails during that time of family harmony.

provided e-mail accounts to its employees. The gallery could not access the employees' passwords or e-mail accounts, but the trustee persuaded the service provider to furnish the passwords, and then she read the employees' correspondence. Among the e-mails reviewed were those between the employees and their attorney. The attorney then brought suit under the SCA. The court dismissed the claim, agreeing that the trustee's access was authorized by the service provider. Id. at *12 (defendant's "access, whether to [the] server or to the e-mails themselves, was authorized by [the service provider]"). The court cited numerous cases in holding that, since the passwords were not secured by fraud or deceit, "the authorization [by the service provider] constitutes a complete defense to liability." Id. Here, Dr. Abadir was authorized by Cablevision, the service provider, to access Plaintiff's account and read her e-mails. Thus, unlike in Connelly, he had consent from both the user (Plaintiff) and the service provider (Cablevision).

d. There was no "Implied Withdrawal" of Consent

Plaintiff has suggested that, even if she initially consented, that consent was impliedly withdrawn when the parties separated. The evidence and the case law demonstrate that Dr. Abadir should prevail as a matter of law on this point as well.

To begin with, Dr. Abadir never voluntarily released control of the Cablevision account. Thus, just as when the couple was married and living together, he did not need Plaintiff's "consent" to access what he believed was his own account. The account remained in Dr. Abadir's name after the parties were separated. Unbeknownst to him, however, Plaintiff, without any authority, called Cablevision and had the account ownership changed to her name.

(Zaratzian Depo. at 57 ln. 13-20, 74 ln. 20 to 75 ln. 8)[5] Surely this unauthorized act did not diminish Dr. Abadir's understanding that he had consent to access the account. Adjusting the facts of Connelly just slightly makes the point: had the attorney there (or the employees) surreptitiously changed ownership of the internet account, it is inconceivable that the trustee would become liable if she continued looking at the e-mails.

The decision in Garcia v. Haskett, 2006 WL 1821232 (N.D. Cal. June 30, 2006), bears this out. The parties there were former law partners who had each maintained an e-mail account under the firm's master account. After the partnership dissolved, the plaintiff took over the computer system, but the defendant continued to log onto the server and read and forward the plaintiff's e-mails. Although the plaintiff alleged that "the Partnership's practice" was that each person was authorized to read only his or her e-mails, the court found that no SCA violation had occurred. The court noted that "Defendant's access of Plaintiff's stored emails was conduct authorized by [the internet service provider]." Id. at *5. It concluded: "To the extent that Plaintiff claims that Defendant violated the Partnership's internal practices, she may have stated a State law claim for violation of a fiduciary duty, but she has not stated a claim for violation of federal law." Id.

Here, too, Dr. Abadir's conduct was authorized by Cablevision (or at least he believed that it was) even after the couple separated since, to his knowledge, the account was in his name. As a result, the court need not reach the issue of withdrawal of consent.

In any event, Plaintiff's earlier consent remained valid because the case law does not recognize an "implied withdrawal" of consent under the facts here. Indeed, New York has

---

[5] In fact, Plaintiff wrongly believed that she was opening a new account in her name, when in fact she merely changed ownership of the existing account. (See Zaratzian Depo. at 65 ln. 8 to 66 ln. 8) She did not learn of her error until 2009. (Id. at 66 ln. 10-11)

specifically rejected the very theory of implied consent that Plaintiff proposes. The couple in Guervich v. Gurevich, 24 Misc. 3d 808 (Kings Cty. Sup. Ct. 2009), was separated, but the wife, without her husband's knowledge, used his e-mail password to access his account and read his correspondence. She then sought to introduce some of the e-mails into evidence in the divorce action. Although the e-mails would have been inadmissible if unlawfully intercepted in violation of New York's analogous wiretapping statute, PL 250.00, the wife contended that her acts were authorized because "[her] husband never formally revoked his permission to look at his e-mails" or "simply chang[ed] his password." Id. at 809. The husband acknowledged that he had not changed his password until "almost two years after the parties physically separated," but, he pointed out, that made it all the more "'shocking' for [his] wife to believe that she had any right to access his account." Id. at 810. And even if she initially had permission to read his e-mails, he argued, "the act of starting a divorce action should constitute, in any event, an implied revocation of such authority." Id. The court ruled for the wife, first holding that the e-mails were not "intercepted" because they were not obtained while "in transit." Id. at 813. Importantly, the court went on to reject the husband's fallback argument, noting that "there is no statute that would recognize an 'implied revocation upon service of a divorce action.'" Id. (emphasis added). This stands as the clearest statement of New York law on this precise point.

The same holds true under federal law. The general rule is that consent can be open-ended, see United States v. Reid, 19 F. Supp. 2d 534, 539 (E.D. Va. 1998)("[s]ince there is no temporal limitation . . . [the] consent was valid until revoked"), and can last for years, see, e.g., United States v. Cantrell, 530 F.3d 684, 691 n.4 (8th Cir 2008)(property owner's general consent to let police officers enter his land was valid two years later). Moreover, "a withdrawal of consent 'can only be accomplished by an unequivocal act or statement.'" United States v.

Masterson, 2009 WL 2365334, at *6 (D. Vt. July 29, 2009)(quoting United States v. Siwek, 453 F.3d 1079, 1086 (8th Cir. 2006)). Accord, United States v. Shaefer, 859 F. Supp. 2d 397, 410 n.14 (E.D.N.Y. 2012)(defendant's act of turning off his computer during search "was not an unequivocal revocation of consent . . . [where], at no point, did defendant state that he no longer gave consent to search and seize the computer"), aff'd, 519 F. App'x 71 (2d Cir. 2013). See also Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000)(revocation of authorization under SCA must be "clear[ ]" and "explicit").

These rules apply with particular force to computers and e-mail accounts, where consent is often open-ended and can extend for very long periods. A case decided just last month demonstrates the point. In Anzaldua v. Northeast Ambulance & Fire Protection District, -- F. Supp. 2d --, 2013 WL 5707875, at *1 (E.D. Mo. Oct. 21, 2013), the plaintiff's ex-girlfriend had "gained access to Plaintiff's private email and passwords" while they were dating. The relationship ended in 2011, but in 2012, she accessed his e-mail account and circulated an embarrassing e-mail he had drafted but not yet sent. In dismissing the plaintiff's SCA claim, the court observed that "the Complaint's allegations raise the question as to whether any access was truly unauthorized, as they indicate [defendant] gained access to Plaintiff's private email and passwords when she was involved in a relationship with Plaintiff, and contain no indication that Plaintiff revoked his consent or authorization before she allegedly accessed the emails." Id. at *10 (emphasis added). That the conduct may have been less than admirable was of no moment, since "'there is no violation . . . for a person with authorized access to the database no matter

how malicious or larcenous his intended use of that access.'" Id. at *11 (quoting Sherman, 94 F. Supp. 2d at 820).[6]

Sherman, a frequently-cited case, reinforces this conclusion. There, counter-plaintiff Salton engaged Sherman to act as a manufacturer's representative to Kmart. Kmart provided Sherman with a computer access code that allowed him to obtain Salton's sales data. Salton then terminated Sherman's contract and instructed Kmart to cut off Sherman's access, but that apparently did not occur until later. In the meantime, Sherman (who was authorized to access the Kmart system for his other clients) continued to use the code to obtain Salton's data. Salton alleged that Sherman "knew he was not so authorized" to continue accessing that information. The court held that the allegations failed to state a claim under the SCA, since withdrawal of previously authorized access must be communicated clearly. Id. at 819. The court explained:

> At a minimum, there must be a clearer and more explicit restriction on the authorized access than [alleged] by Salton[] .... Here Sherman's access to the Salton data in the Kmart network system was in no way restricted by technical means or by any express limitation .... Salton admits that Kmart provided Sherman with authorization to log on to the computer network to access information about vendors and products that Sherman was representing. Further, Kmart continued to provide James Sherman access to Salton's information after his dismissal by Salton. Salton has not pled or offered to show that Kmart instructed Sherman that he no longer had authorization to access sales information.

Id. at 821. Accordingly, the court held that Salton had failed to allege specific facts to state a violation of the SCA.

---

[6] The court in Clarity used similar reasoning to grant summary judgment on an SCA claim. The employee there continued to access his e-mail after he had resigned his position but before the account was suspended. This was held not unlawful because (i) the initial access was authorized and (ii) the employee "retained full access to the . . . account" during the interregnum. 698 F. Supp. 2d at 1316.

These words easily could have been written to describe the deficiencies in Plaintiff's proof. As in Sherman, Dr. Abadir's initial access to Plaintiff's e-mail account was authorized, and there is no evidence that Plaintiff ever communicated to Dr. Abadir a "clear[]" and "explicit restriction" on that authorization (or, indeed, any restriction). Nor was Dr. Abadir's access to the Optimum On-Line network "restricted by technical means or by any express limitation." To the contrary, Dr. Abadir used his own computer and his own password to log onto the system and to access his own account. And Plaintiff has not adduced evidence that Cablevision "instructed" Dr. Abadir that "he no longer had authorization" to access his account. In fact, she acknowledges that the e-mail forwarding ceased immediately when she provided clear instructions to Cablevision to close down his account. (SAC ¶14)

Finally, it is significant that Dr. Abadir did not access his wife's account after the couple separated. Indeed, Plaintiff's theory is that he accessed his own account and read his own e-mails. He did not look at or adjust her account settings, nor did he enter her password and thereby review her correspondence. Exhaustive research has failed to reveal any case in which authorized conduct (here, the setting of the auto-forward rule while the parties were together) morphed into illegality when the parties separated, even if the defendant continued to receive the fruits of his early conduct. As noted above, the Second Circuit has strongly cautioned lower courts against turning domestic disputes into criminal surveillance violations. That policy, together with the rule of lenity, means that any lingering ambiguity here should be resolved in Dr. Abadir's favor.

iii. There Was No "Interception" Here

Dr. Abadir also did not violate the Wiretap Act because he did not "intercept" any electronic communications. As explained below, the law distinguishes between electronic

communications in transit (which can be "intercepted" under the Wiretap Act) and electronic communications "in storage" (which cannot). Dr. Abadir set an "auto-forwarding" rule on Plaintiff's e-mail account so that he would receive copies of all of her incoming e-mail messages. That rule is implemented only after the destination server has received and stored the e-mail. As the plain statutory language and the majority of cases make clear, electronic communications stored on a destination server are no longer "in transit" and cannot be "intercepted" within the meaning of the Wiretap Act. See, e.g., Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148 (C.D. Cal. 2007)(configuring server software to auto-forward e-mail messages is not "interception" under Wiretap Act since routing occurs only after messages are stored on destination server). At most, then, Dr. Abadir "accessed" an electronic communication while it was in "storage," and Plaintiff's claim must be analyzed under the SCA and not the Wiretap Act.

a. The Facts

Cablevision witness Timothy Chase described the mechanics of Optimum On-Line's auto-forwarding rule. Once a user creates an e-mail and clicks "send," the e-mail is sent to a mail transfer agent ("MTA"). (Chase Depo. at 20 ln. 3-9) The MTA -- an application or program that runs on a server -- determines the recipient network, opens a connection with that network, and sends the e-mail. (Id. at 20 ln. 8-12)

Before sending the message, however, the operating system on the originating server breaks down the message into smaller "packets." (Id. at 25 ln. 9-16; 26 ln. 9-13) The packets are then transmitted to the destination server, which reassembles them. (See id. at 26 ln. 13-18) The MTA on the destination server reviews the e-mail and determines what to do with it. (See id. at 27, ln. 5-8) Among other things, the MTA implements any rule (such as an auto-forwarding rule) that has been set. (See id. at 35 ln. 23 to 36 ln. 24) When that occurs, the e-

mail resides on the destination server, with copies sent to the original recipient and to the forwarded recipient. (See id. at 35 ln. 23 to 39 ln. 12). In sum, the auto-forwarding rule is implemented only after the e-mail has been received, reassembled, and stored by the server.

b. The Law of "Interception"

The Wiretap Act makes it unlawful for a person intentionally "to intercept any wire, oral or electronic communication." 18 U.S.C. §2511(1)(a). The statute defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). An electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. §2510(12).

The term "intercept" has been given a narrow construction. See Konop, 302 F.3d at 878 ("When Congress passed the USA PATRIOT Act, it was aware of the narrow definition that courts had given the term 'intercept' with respect to electronic communication, but chose not to change or modify that definition"); see also Fredrick v. Oldham County Fiscal Court, 2010 WL 2572815, at *2 (W.D. Ky. Jun. 23, 2010)(although, "in layman's terms, the act of accessing and forwarding an e-mail from another's e-mail account could be understood as an 'intercept,' cases interpreting this term have given the word a much narrower definition"). Generally, courts find that an "interception" of electronic communications can happen "only where the acquisition of the communication occurs contemporaneously with its transmission by its sender." Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009)(emphasis added); see also Konop, 302 F.3d at 877; United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996).

As the Global Policy Court helpfully explained:

> "[I]ntercept" . . . is perhaps best understood through a football analogy. In American football, a ball can only be intercepted when it is "in flight." Once a pass receiver on the offensive team has caught the ball, the window for interception has closed, and the defenders can only hope to force a fumble. In essentially the same way, a qualifying "intercept" under the [Wiretap Act] can only occur where an e-mail communication is accessed at some point between the time the communication is sent and the time it is received by the destination server . . . .

686 F. Supp. 2d 638 (emphasis added); see also Fredrick, 2010 WL 2572815, at *3 (endorsing football analogy).

In other words, once an electronic communication has reached its destination, it is no longer "in flight" but, rather, is "in storage." Any access to it thus falls under the SCA and not the Wiretap Act. See Konop, 302 F.3d at 877 (if electronic communication is in transit it may be "intercepted" in violation of Wiretap Act, but it is not "stored" for purposes of SCA; conversely, stored computer information may be unlawfully "accessed" in violation of SCA, but it cannot be "intercepted" for purposes of Wiretap Act). Simply put, it is not an interception to access electronic communications that are in storage. See e.g., Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2004); United States v. Steiger, 318 F.3d 1039, 1046-47 (11th Cir. 2003); Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004)(accessing e-mails stored by plaintiff's internet service provider was not an interception); Garback v. Lossing, 2010 WL 3733971, at *2 (E.D. Mich. Sept. 20, 2010)(Congress intended for electronic communications in storage to be handled solely by SCA).

The line between electronic communications "in flight" (which are subject to interception) and "in storage" (which are not) finds its roots in the legislative history of the two statutes. In 1986, Title I of the Electronic Communications Privacy Act amended the Wiretap

Act (which until then had addressed only the interception of wire and oral communications) to include the interception of electronic communications. See Konop 302 F.3d at 874 (citing Pub.L. No. 99-508, 100 Stat. 1848; S.Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557). At the same time, Title II of the ECPA created the Stored Communications Act to address wire and electronic communications in storage. See id. Importantly for our purposes, Congress included electronic storage in the definition of "wire communication," but not in the definition of "electronic communication." Compare 18 U.S.C. §2510(1)(defining "wire communication") with 18 U.S.C. §2510(12)(defining "electronic communication"). As courts have observed, this difference underscored Congress' belief that one can "intercept" a wire communication -- but not an electronic communication -- that resides in storage. See Steiger, 318 F.3d at 1048; Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461-62 (5th Cir. 1994)(definitional difference indicates that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage'").[7]

Congress clarified this point in the USA PATRIOT Act of 2001, which amended the Wiretap Act by eliminating "storage" from the definition of "wire communication." See

---

[7] As the Fifth Circuit explained in Steve Jackson Games, the reason that interception applies only to a narrow category of electronic communications may be best understood in the context of law enforcement. The government may access electronic communications in storage for less than 180 days by obtaining a warrant, but there are "stringent, complicated requirements for the interception of electronic communications; a court order is required." 36 F.3d at 463 (citing 18 U.S.C. §2703(a) and 18 U.S.C. §2518). Moreover, court orders authorizing interception are subject to other requirements, "such as those governing minimization, duration, and the types of crimes that may be investigated," that are not imposed when the government seeks access to stored communications. Id.; see also Mogerman, C.J. and Jones, S.L., "The New Era of Electronic Eavesdropping and Divorce: An Analysis of the Federal Law Relating to Eavesdropping and Privacy in the Internet Age," 21 J. Am. Acad. Matrim. Law 481, 485-86 (2008)(Congress viewed "interception" as vastly different from accessing stored communication and intended the former to be more highly policed).

Steiger, 318 F.3d at 1048 (change meant to reduce protection of voice mail messages to that afforded other electronically stored communications). As the Ninth Circuit explained in Konop:

> When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission.

302 F.3d at 878 (citations omitted).

As a result of these amendments, it is now recognized that "very few seizures of electronic communications from computers will constitute 'interceptions.'" Steiger, 318 F.3d at 1050; see also Garback, 2010 WL 3733971, at *3 ("interception of email can occur in only a very narrow range of circumstances"). This does not create a statutory lacuna, but merely relegates the vast majority of plaintiffs to their remedies under the SCA rather than the Wiretap Act. See Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 980-81 (M.D. Tenn. 2008)("Simply because e-mail is not readily susceptible to "interception" does not mean that the courts should bend the language of the statute so it provides an additional avenue of relief to a supposedly aggrieved party. Congress has provided a remedy for the individual whose e-mails are accessed in an unauthorized way-the SCA.").[8]

The question therefore becomes: when is an e-mail in "electronic storage" and thus not susceptible to "interception" under the Wiretap Act? The answer, not surprisingly, lies in the plain language of the ECPA, which broadly defines "electronic storage" to mean "(A) any

---

[8] In Hall v. Earthlink Network, Inc., 396 F.3d 500 (2d Cir. 2005), the Second Circuit cited Fraser, Steiger, Konop and Steve Jackson Games with approval, thereby endorsing the prevailing line of cases differentiating electronic communications "in transit" (and therefore subject to interception under the Wiretap Act) from those "in storage" (which are not). See Hall, 396 F.3d at 503 n.1, 504.

temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. §2510(17)(emphasis added). Accordingly, when an e-mail rests even for a fleeting moment in electronic storage -- during its transmission to another server, when it reaches that server, or otherwise -- its access must be evaluated under the SCA. See, e.g., Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007)(information in temporary storage in RAM cannot be "intercepted"). In other words, although "the transmission time of email messages is very short, as it travels through wires 'at the speed of light' . . . the duration of the storage of the electronic communication is immaterial." Bunnell v. Motion Pictures Ass'n of America, 567 F. Supp. 2d 1148, 1152 (C.D. Cal. 2007). As a result, "[e]ven if the storage phase is transitory and lasts only a few seconds, it is still considered 'electronic storage' under the ECPA." Id.; see also Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417, 431 (S.D.N.Y. 2010). As commentators have described it: "an e-mail is only an electronic communication when it is not in electronic storage. Throughout the transmission process, an e-mail can float in and out of the definition several times. Given the speed within which the transmission process occurs, there is very little protection for electronic communications." Mogerman and Jones, supra n.7, at 489.

Thus, courts have found: (i) that e-mail messages on an electronic bulletin board that had not yet been accessed by the intended recipients were "in storage" such that the government's seizure of the computer used to operate the electronic bulletin board was not an unlawful intercept under the Wiretap Act, Steve Jackson Games, 36 F.3d at 464 n.10; (ii) that electronic communications on a provider's server were "in storage" even though they had not yet

been accessed by the intended recipient, Theofel v. Farley-Jones, 359 F.3d 1066 (9th Cir. 2004); and (iii) that no interception had occurred where e-mails "had reached their destination server," Global Policy, 686 F. Supp. 2d at 639; Fredrick, 2010 WL 2572815, at *3 ("interception" requires accessing electronic communication before it is received by destination server).

The court in Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148 (C.D. Cal. 2007), applied these rules in circumstances very similar to those here. It found that enabling an e-mail auto-forward feature was not an interception under the Wiretap Act because the e-mails were necessarily "stored" before they were forwarded:

> Anderson configured the Bunnell parties' email server software so that all Plaintiffs' messages were copied and forwarded from the server to his Google email account. If the emails had not been stored on the server, Anderson would not have acquired copies of them.

Id. at 1153 (emphasis added). The court noted that the word "intercept" means "to stop, seize, or interrupt in progress or course before arrival." Id. at 1154 (citing Konop, 302 F.3d at 878, and Webster's Ninth New Collegiate Dictionary 630 (1985)). Because the auto-forwarding feature "did not stop or seize any of the messages that were forwarded to him[,] Anderson's actions did not halt the transmission of the messages to their intended recipients." Id. Thus, "under well-settled case law, as well as a reading of the statute and the ordinary meaning of the word 'intercept,' Anderson's acquisition of the emails did not violate the Wiretap Act." Id.

The facts (and the result) in Executive Security Management, Inc. v. Dahl, 830 F. Supp. 2d 883 (C.D. Cal. 2011), were also similar. The defendants there surreptitiously configured settings to cause copies of e-mails to be forwarded to their accounts. Citing Bunnell, the court observed that the auto-forwarding did not "stop or seize any of the messages" or "halt the transmission of the messages to their intended recipients." Id. at 904. Therefore, the facts

were "insufficient to demonstrate an 'intercept[ion]' under the narrow reading of the Wiretap Act's use of that word." Id. at 905; see also Fredrick, 2010 WL 2572815, at *2 ("[t]hough, in layman's terms, the act of accessing and forwarding an e-mail from another's e-mail account could be understood as an 'intercept,' cases interpreting this term have given the word a much narrower definition").[9]

c. There was No "Interception" Under the Undisputed Facts Here

Under the prevailing view of the law, Dr. Abadir did not "intercept" any electronic communications because he did not "stop," "seize" or "halt" any messages directed to azaratzian@optonline.net. As Chase testified, the auto-forwarding rule here was implemented only after the e-mail message has been received and reassembled by the destination server. At

---

[9] A minority of courts have reached a different conclusion. In United States v. Councilman, 418 F.3d 67 (1st Cir. 2005)(en banc), a divided First Circuit found that electronic communications in "transient storage" incidental to their transmission could still be "intercepted" under the Wiretap Act. See id. at 79 ("an e-mail message does not cease to be an 'electronic communication' during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage"). Likewise, in United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010), the Seventh Circuit held that the secret planting of an auto-forwarding rule yielded an interception under the Wiretap Act. These courts reached their conclusion only by reading language into the statute. Councilman, for example, broadened the definition of "electronic communication" by stating that it "includes transient electronic storage that is intrinsic to the communication process for such communications." 418 F.3d at 79. However, as the dissent in Councilman noted:

> It is not by coincidence that every court that has passed upon the issue before us has reached a conclusion opposite to that of the en banc majority: that the Wiretap Act's prohibition on intercepting electronic communications does not apply when they are contained in electronic storage, whether such storage occurs pre-or-post-delivery, and even if the storage lasts only a few mili-seconds.

Id. at 87 (Torruella, J., dissenting). See also Serwin, Andrew B., "Information Security & Privacy: A Guide to Federal & State Law & Compliance," §7:24 (describing Councilman as the minority view).

that point, the e-mail was stored on the destination server, which made copies of it and distributed it as per its protocol. In other words, the e-mail was no longer "in transit" and could not be "intercepted." Or, using the football analogy, it was caught by the intended receiver and then fumbled.[10]

Finally, the rule of lenity requires that any remaining ambiguity be resolved in Dr. Abadir's favor. If one thing is certain, it is that this area of law is hypertechnical, often counterintuitive, and in flux. Moreover, it has yielded a variety of approaches to even the most basic issues, producing a confusing array of judicial opinions. The Konop Court correctly observed as follows:

> [T]he intersection of [the Wiretap Act and the SCA] "is a complex, often convoluted, area of the law." United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998). . . . [T]he difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communications . . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. . . . We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . . will remain a confusing and uncertain area of the law.

302 F.3d at 874. See also Serwin, supra n.9, at §7:24 (despite prevailing view that communications can only be intercepted while "in flight," "courts continue to be somewhat

---

[10] Judge Motz recognized as much in ruling on Defendants' motions to dismiss in this case, writing, "Dr. Abadir's arguments may well be meritorious." Docket 25 at 2 (emphasis added). He agreed that an "interception" "does not occur unless the defendant interposes himself between the sender and the recipient to obtain the electronic communication while it is in transit." Id. And he noted that the leading cases were endorsed by the Second Circuit in Hall v. Earthlink Network, Inc., 396 F.3d 500 (2d Cir. 2005). He denied the motion only because he found that "it does not seem that the scope of discovery will be broadened in any respect by denial of the motion as to count one and therefore, from the perspective of efficient case management, it is advisable to defer ruling upon the issues raised by Dr. Abadir's motion to dismiss count one until a later stage of this litigation." Id.

confused by these issues"). These are precisely the circumstances where the rule of lenity offers a defendant the benefit of the doubt.

d. The Statute of Limitations Has Run

The Wiretap Act claim should also be dismissed because the statute of limitations has expired. Civil actions under the Act "may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation." 18 U.S.C. §2520(e). Like many statutes of limitation, "this one does not require the claimant to have actual knowledge of the violation; it demands only that the claimant have had a reasonable opportunity to discover it." Davis v. Zirkelbach, 149 F.3d 614, 618 (7th Cir. 1998). For this reason, "inquiry notice" is sufficient to commence the running of the statute of limitations. Id.; see also Steinbach v. Village of Forest Park, 2009 WL 2857302, at *1 (N.D. Ill. Aug. 5, 2009)(statute began to run when plaintiff became aware that someone had accessed her e-mail account without authorization, not when she learned that defendant had logged into her account and read an e-mail). Plaintiff filed her initial Complaint on December 6, 2010, more than two years after she had a "reasonable opportunity" to discover any alleged violation.

Plaintiff acknowledged in her deposition that there were "a lot of things [that] happened that raised [her] suspicion" that Dr. Abadir was improperly reading her e-mail (Zaratzian Depo. at 101 ln. 5-7), some of which occurred more than two years before she filed the Complaint. Indeed, he seemed to know so much that she first speculated whether "the neighbors were spying on [her]." (Zaratzian Depo. at 103)("I didn't understand how he knew all these little things about me that he shouldn't have known."). As events unfolded, however, she concluded that he was reading her e-mails.

For example, on November 11, 2007, Dr. Abadir e-mailed Plaintiff that, "[a]t my last count, the kids have been exposed to 3 of your significant others in the past several months." (Zaratzian Depo. Ex. 8) Plaintiff found this suspicious because the children had not, in fact, met the men that she had dated. (See Zaratzian Depo. at 101; Plaintiff's Response to Defendant's Second Set of Interrogatories, dated November 7, 2011, at ¶1 ("Outside of email communications, no one knew [I] had dated three men.")) She concluded that Dr. Abadir's knowledge was so specific that he must have been reading her e-mails. As she testified, "the fact that he knew I was dating three men meant that he was looking at my e-mails." (Id.) And, as noted above, Plaintiff had changed her password years before, and thus Dr. Abadir must have had some other way to read her e-mail. Nevertheless, Plaintiff took no action at the time to discover how her husband was "looking at [her] e-mails." (Zaratzian Depo. at 112 ln. 14)

Another red flag was raised in early 2008, when Harold Burke (her then boyfriend) forwarded an e-mail to her from his ex-wife in which his ex-wife described him as an "ADD Loser Idiot." (Zaratzian Depo. at 99) Then, in the summer or fall of 2008, Tanya (the couple's daughter) related a conversation in which Dr. Abadir had used that very same phrase to describe Mr. Burke. When Plaintiff heard this, she reasonably (and correctly) suspected that Dr. Abadir was reading her e-mails. She testified as follows:

> Q: Did you think that Dr. Abadir had somehow seen that email?
>
> A: I didn't waste a lot of time thinking about how he got it and how he used it. A lot of things had happened that raised my suspicion, but nothing could be proved.
>
> * * *
>
> Q: Did you think that there was some way that Dr. Abadir could know the phrase "ADD loser idiot" without having seen that email?

A: No.

Q: So when you heard Tanya say that to you, did you think that Dr. Abadir had seen that email?

A: I did.

(Zaratzian Depo. at 101 ln. 3-6, 103 ln. 19-24).

Again, despite the fact that her ex-husband had quoted verbatim from an e-mail to which she believed he had no legitimate access, Plaintiff took no further action to determine how he had been able to see this very private correspondence. The question, of course, was not whether something "could be proved" (though a simple call to Cablevision would have resolved the matter), but whether Plaintiff was on inquiry notice that her e-mail account had been compromised. That Plaintiff chose not to "waste a lot of time thinking about how he got it" underscores the limited importance she put on her e-mail privacy at that time. It also shows a lack of diligence in discovering facts that would have led her to file her lawsuit earlier. After all, an ex-wife in the midst of contentious custody proceedings who has twice concluded that her ex-husband has been reading her private e-mails has sufficient information to be on inquiry notice that he had somehow gained visibility into her account.

Nevertheless, despite being aware as early as 2007 that "something was afoot," Davis, 149 F.3d at 618, a suspicion that was reinforced in mid-2008, Plaintiff did not bother to investigate how Dr. Abadir could have been seeing her e-mails until June 2010. At that time, she called Cablevision and learned that an auto-forwarding rule was in place on her e-mail account, demonstrating that only a little legwork was required to ascertain what had occurred. Because she waited more than two years to file her Complaint after having "a reasonable opportunity to discover" the intrusion, however, Plaintiff cannot be heard to argue that her lawsuit is timely.

* * *

For the above reasons, the Court should grant summary judgment and dismiss Count One of the SAC.

C. There was No Stored Communications Act Violation

For many of the same reasons as set forth above, Dr. Abadir did not violate the SCA. That statute requires proof that a person "(1) intentionally accesse[d] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[ed] an authorization to access that facility; . . . and thereby obtain[ed] . . . . [un]authorized access to a[n] . . . electronic communication while it [was] in electronic storage." 18 U.S.C. §2701(a). As discussed above, Plaintiff shared her password with her then-husband, thereby authorizing him to read and monitor her e-mail account, and she never withdrew that authorization. Moreover, the same two-year statute of limitations, with the same "inquiry notice" qualification, applies to the SCA, see §2707(f), and thus this claim is likewise untimely.

There is an even more fundamental reason, however, why the SCA claim should be dismissed: Dr. Abadir never accessed Plaintiff's account. The SCA addresses computer "hacking", namely the unauthorized access to the account of another. It does not prohibit one from logging onto his own e-mail account, as Dr. Abadir did here. Indeed, §2701(c) specifically states that no violation occurs if the access was authorized "by the person or entity providing a wire or electronic communications service."

In Connelly, a court in this district relied on §2701(c) in granting summary judgment in favor of the art gallery trustee who was accused of reading employees' e-mails. The court held that there could be no SCA violation because the service provider had granted the trustee access to those e-mail accounts. Absent fraud upon the provider, the court observed, "the authorization [by the provider] constitutes a complete defense to liability." Id. at *12 (citing

cases). Here, Cablevision authorized Dr. Abadir to log onto his e-mail account, and there is no proof (or even the allegation) that he used fraud or deceit to persuade it do so.[11]

The cases validating SCA claims make clear that the statute prohibits accessing another's account by improper means -- conduct that is simply not present here. See, e.g., Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 202-03 (4th Cir. 2009)(employer hacked into former employee's personal e-mail account); Theofel v. Farey-Jones, 359 F.3d 1066, 1073 (9th Cir. 2004)(invalid subpoena used to gain access to another's stored e-mails); Pure Power Boot Camp Inc. v. Warrior Fitness Boot Camp LLC, 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008)(employer used employee's user name and password to access employee's personal e-mail account); Bloomington-Normal Seating Co., Inc. v. Albritton, 2009 WL 1329123, at *3 (C.D. Ill. May 13, 2009)(employee hacked into manager's e-mail account); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 977 (M.D. Tenn. 2008)(former employee used ex-co-worker's user name and password to access e-mail account); Bailey v. Bailey, 2008 WL 324156, at *5 (E.D. Mich. Feb. 6, 2008)(husband obtained wife's e-mail password with key-logging software and then accessed her account to read her messages). Notably, research has not uncovered any case where a defendant has been found liable under the SCA for using his own authorized password to obtain access to his own e-mail account, which is precisely what occurred here.

Accordingly, the Court should grant summary judgment on Plaintiff's SCA claim as well.

---

[11] The privacy intrusion in Connelly was even more substantial than that here, since the trustee did not merely access her own account, but learned the passwords for the employees and accessed their accounts.

POINT II

THE COURT SHOULD GRANT SUMMARY JUDGMENT ON THE CONSTRUCTIVE FRAUD BY FIDUCIARY CLAIM

In Count Five of the SAC, Plaintiff asserts a state-law claim styled "Constructive Fraud by Fiduciary." The essence of the claim is that Dr. Abadir breached "his fiduciary duty" to Plaintiff by failing to inform her during the negotiation of their marital separation agreement that he was receiving copies of her incoming e-mail, including e-mails with her matrimonial attorney; and by using the information he derived to gain an unfair financial advantage in the agreement. (SAC ¶¶57-58) Like Plaintiff's federal claims, this claim also should be dismissed.

As a threshold matter, this court only has supplemental jurisdiction over the claim, 18 U.S.C. §1367(a), and it should decline to exercise this jurisdiction if it dismisses Counts One and Two. Id. §1367(c)(3)("district courts may decline to exercise supplemental jurisdiction over a claim under subsection (a) if . . . the district court has dismissed all claims over which it has original jurisdiction"). See Castiglione v. Papa, 423 F. App'x 10, 13 (2d Cir. 2011)("Having dismissed [plaintiff's] only federal law claims, the District Court should have declined to exercise supplemental jurisdiction over her remaining state law claims."). In any event, the claim cannot withstand summary judgment on the merits.

"A fiduciary relationship exists between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation. . . . It exists only when a person reposes a high level of confidence and reliance in another, who thereby exercises control and dominance over him." People ex rel. Cuomo v. Coventry First LLC, 13 N.Y.3d 108, 115, 886 N.Y.S.2d 671, 675 (2009)(internal quotation marks and citations omitted). See also Varveris v. Zacharakos, 110 A.D.3d 1059, 1059, 973 N.Y.S.2d 774, 775 (2d Dep't 2013)(fiduciary relationship exists between two persons only

"when one of them is under a duty to act for . . . the benefit of another upon matters within the scope of the relation")(quotation omitted). Moreover, "marriage . . . alone, does not create a fiduciary relationship." Infanti v. Scharpf, 2012 WL 511568, at *8 (E.D.N.Y. Feb. 15, 2012)(citing United States v. Chestman, 947 F.2d 551, 568 (2d Cir.1991)). Even in marriage, a fiduciary relationship requires "reliance, and de facto control and dominance, . . . or . . . repeated disclosure of business secrets between the spouses." Id. (citations and internal quotation marks omitted).

At the relevant time here, the parties were divorcing -- indeed, it is their divorce proceeding that Plaintiff asserts was tainted as a result of Dr. Abadir's having received Plaintiff's e-mails. Under these circumstances, Dr. Abadir was not under a duty to act for Plaintiff's benefit so as to create a fiduciary relationship. To the contrary, Plaintiff and Dr. Abadir were opposing litigants in a hotly-contested divorce, which surely is the antithesis of a fiduciary relationship. The claim of fraud by a fiduciary thus fails as a matter of law on the absence of a fiduciary relationship.

Moreover, Plaintiff has produced no evidence to support her contention that Dr. Abadir's access to her e-mails adversely affected the outcome of the divorce. As she testified at her deposition:

> Q: My question is, how were you damaged by what you describe in [paragraphs] 50 through 59 [of the Complaint]?
>
> A: He was reading my emails to my lawyer. And to my lawyer, I communicated what had been discussed . . . . And I don't know exactly what happened or what transpired, but I do know that he should not have had access to them. And he did.
>
> Q: And --
>
> A: And I can only surmise that had it not been for that, I might have gotten a clean trial. The fact that he had knowledge hurt

> me, I'm sure. I don't exactly know in what way. I'm sure that he put -- I mean, I'm speculating at this point.
>
> * * *
>
> Q. . . . So what information, in particular, are you claiming led to the unfair settlement?
>
> A: He saw all my attorney-client communications. Not all, but whatever was on the thread. He saw enough of it.
>
> Q: So what specifically --
>
> A: I don't know specifically.
>
> * * *
>
> Q: So my question is, what emails did you receive from your lawyer that you believe resulted in you getting an unfair settlement by the fact that they were forwarded to Dr. Abadir?
>
> A: I don't recall specifically.

(Zaratzian Depo. at 115 ln. 13 to 116 ln. 5; 118 ln. 12-18; 118 ln. 24 to 119 ln. 4)(emphasis added). Plaintiff further conceded that she could not identify any e-mails seen by Dr. Abadir that involved (i) the matrimonial proceedings' disposition of the couple's home (122:5-9); (ii) distribution of assets, child support, child custody or alimony (123 ln. 9-14); or (iii) communications generally between Plaintiff and her lawyer "about the settlement parameters" (124 ln. 7-11).

In short, despite Plaintiff's high-sounding allegations that Dr. Abadir's access to her e-mails with counsel compromised her matrimonial settlement, she was forced to admit that her claim is premised on mere "surmise" and "speculat[ion]." Much more is necessary to defeat a motion for summary judgment.

POINT III

THE COURT SHOULD GRANT SUMMARY JUDGMENT ON THE REQUESTS FOR INJUNCTIVE RELIEF

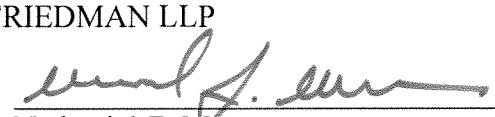
In Count Six of the SAC, Plaintiff seeks injunctive relief based on the alleged violations of the Wiretap Act and the Stored Communications Act. Because Plaintiff has failed to sustain these claims, Count Six should be dismissed as well.

CONCLUSION

For the reasons stated above, the Court should grant summary judgment and dismiss the Complaint in its entirety.

Dated: New York, New York
November 22, 2013

BALLARD SPAHR STILLMAN & FRIEDMAN LLP

By: 

Nathaniel Z. Marmur
Mary Margulis-Ohnuma
425 Park Avenue
New York, New York 10022
(212) 223-0200
MarmurN@bssfny.com
OhnumaM@bssfny.com

Attorneys for Defendant Adel Ramsey Abadir